

Erinnerung:

Eine Menge G , zusammen mit einer
Abbildung $G \times G \xrightarrow{(\cdot)} G, (g, h) \mapsto g \cdot h$,
heißt **Gruppe**, falls

- $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ für $g, h, k \in G$
- $\exists 1 = 1_G \in G$ mit $1 \cdot g = g$
und $g \cdot 1 = g$ für $g \in G$

Es liegt 1_G eindeutig fest.

- $\forall g \in G \exists g^{-1} = g^{-1} \in G$ mit
 $g \cdot g^{-1} = 1_G$
 $g^{-1} \cdot g = 1_G$

Für $g \in G$ liegt g^{-1} eindeutig fest.

Beispiele : • Symmetrische Gruppe S_n auch: $\{1, \dots, n\}$
auf einer Menge Ω ✓
- z.B. $S_{\{1, \dots, n\}} =: S_n$ für $n \geq 0$

- $GL_n(K)$ für Körper K und $n \geq 0$
- Untergruppen davon

G : Gruppe

Π : Menge

symmetrischer Gruppe auf Π

• $\alpha: G \rightarrow S_\Pi$ Gruppenhomomorphismus

$\leadsto \Pi = (\Pi, \alpha)$ ist G -Menge

$$g \cdot u := (\alpha(g))(u)$$

• Zugang via Repräsentationsabbildung:

Sei $G \times \Pi \rightarrow \Pi$
 $(g, u) \mapsto g \cdot u$

mit $\begin{cases} 1 \cdot u = u & \text{für } u \in \Pi \\ (g \cdot h) \cdot u = g \cdot (h \cdot u) & \text{für } g, h \in G, u \in \Pi \end{cases}$

$$\Rightarrow (\alpha(g))(u) := g \cdot u$$

$$\Rightarrow \Pi = (\Pi, \alpha) \text{ ist } G\text{-Menge}$$

Operator α injektiv

Bsp

• $U \leq S_n \Rightarrow [1, n]$ ist treue

symmetrischer Gruppe, $n \geq 0$

U -Menge

mit $u \cdot k = u(k)$

• $U \leq G$

$$\Rightarrow G/U = \{hU : h \in G\}$$

ist G -Menge mit $g \cdot (hU) := (gh)U$
 für $g \in G$ und $h \in G$

G : Gruppe

Π, N : G -Mengen

- $\Pi \xrightarrow{f} N$ heißt **G -Abbildung**,
falls $f(g \cdot u) = g \cdot f(u)$ für $g \in G, u \in \Pi$

- Ist die G -Abbildung f bijektiv, so heißt
sie **G -Bijektion** oder **Isomorphismus von G -Mengen**.

- $u \in \Pi \Rightarrow G \cdot u = \{g \cdot u : g \in G\} \subseteq \Pi$
heißt **Bahn** von u

- Disjunkte Zerlegung: $\Pi = \bigcup_{i \in [1, k]} G u_i$,
wobei $\{u_1, \dots, u_k\}$ gewählte
Repräsentantenmenge der Bahnen.

$k \geq 0$

- $\Pi^{\times k} = \{(u_i)_{i \in [1, k]} : u_i \in \Pi \text{ für } i \in [1, k]\}$
ist G -Menge vda $g \cdot (u_i)_i := (g \cdot u_i)_i$
- $\Pi^{\times k, \neq} = \{(u_i)_i \in \Pi^{\times k} : u_i \neq u_j \text{ falls } i \neq j\}$
ist G -Teilmenge in $\Pi^{\times k}$

G : Gruppe

Ω : G -Menge

Ω heißt **transitiv**, wenn Ω aus genau einer Bahn besteht. D.h. wenn $\Omega = G\omega$ für $\omega \in \Omega$.

$k \geq 0$

Ω heißt **k -fach transitiv**, wenn $\Omega^{\times k} \neq \emptyset$

transitiv ist.

Bsp: Die S_n -Menge $[1, n]$ ist n -fach transitiv.

Bahnenlemma: $\omega \in \Omega$

$$C_G(\omega) = \{g \in G : g \cdot \omega = \omega\}$$

Stabilisator

G -Bijektion:

$$\begin{array}{ccc} G/C_G(\omega) & \xrightarrow{\sim} & G \cdot \omega \\ gC_G(\omega) & \mapsto & g \cdot \omega \end{array}$$

Lemma 2.2 Ω : transitive G -Menge, T : G -Menge
 $\Omega \xrightarrow{f} T$ surj. G -Abbildung
 $\omega \in \Omega$

(1) $C_G(\omega) \leq C_G(f\omega) \leq G$

(2) $C_G(\omega) = C_G(f\omega) \iff f$ bij.

(3) $C_G(f\omega) = G \iff T$ trivial

note!
??

G : Gruppe

Π : transitiver G -Menge

• Sei Π nichttrivial.

Es heißt Π **primär**, falls

$\Pi \xrightarrow[\substack{\text{surj.} \\ G\text{-Abb.}}]{f} T \implies f \text{ bijektiv oder } T \text{ trivial}$

• $B \subseteq \Pi$ heißt **Block**, falls $gB = B$ oder $gB \cap B = \emptyset$ für $g \in G$.

Lemma 2.8

Π transitiv und nichttrivial.

Äquivalent sind:

(1) Π ist primär

(2) Es gibt auf Π keine G -Äquivalenzrelation, die weder diskret noch vollständig ist

(3) Es gibt in Π keinen Block B mit

$|B| > 1$ und $B \subseteq \Pi$

(4) $\exists m \in \Pi$ mit: $C_G(m) \stackrel{\max}{<} G$

(5) $\forall m \in \Pi$ ist: $C_G(m) \stackrel{\max}{<} G$

Bew.

(4) $\iff$ (5) $\iff$ (1) $\iff$ (2) $\iff$ (3)

G : endliche unendl. Gruppe

$S \subseteq G$: endl. Teilmenge mit $G = \langle S \rangle$

$$S^{\pm} := S \cup \{s^{-1} : s \in S, | \langle S \rangle | = \infty\}$$

$\uparrow$ Falls G endlich, dann $S^{\pm} = S$

Jedes Element von $G = \langle S \rangle$ kann also
als Produkt von Elementen aus $S^{\pm}$ geschrieben
werden.

Π : G -Menge

$u \in \Pi$: Element mit $G \cdot u = \{g \cdot u : g \in G\}$
endlich. $\leftarrow$ z.B.: Π endlich,
 $u \in \Pi$ beliebig

Wollen: $G \cdot u = \{g \cdot u : g \in G\}$

und

$$C_G(u) = \{g \in G : g \cdot u = u\}$$

sparsam berechnen

(Erzeuger für $C_G(u)$)

Bsp:

$$G = \langle \overset{=:a}{(1,2,3)}, \overset{=:b}{(3,4,5)} \rangle$$

$$\leq S_6$$

$$\Pi = \{1, 2, 3, 4, 5, 6\}$$

$$u = 3$$

7

① Nicht in Kästen:

$$G \cdot 3 = \{1, 2, 3, 4, 5\}$$

② In Kästen:

$$\text{II} : \tau(b a a)^{-1} \circ (b a a)$$

$$= a^{-1} \circ b \circ a = (2, 4, 5)$$

$$\text{IV} : \tau(a b b)^{-1} \circ (a b b)$$

$$= b^{-1} \circ a \circ b = (1, 2, 5)$$

$$\text{III} : \tau(a^3)^{-1} \circ a^3$$

$$= \text{id}^{-1} \circ a^3 = \text{id}$$

$$\text{VI} : \tau(b \circ a^2)^{-1} \circ b \circ a^2$$

$$= (a^2)^{-1} \circ b \circ a^2 = (1, 4, 5)$$

$$\text{V} : \tau(a \circ b^2)^{-1} \circ a \circ b^2$$

$$= (b^2)^{-1} \circ a \circ b^2 = (1, 2, 4)$$

$$\text{VII} : \tau(b^3)^{-1} \circ b^3$$

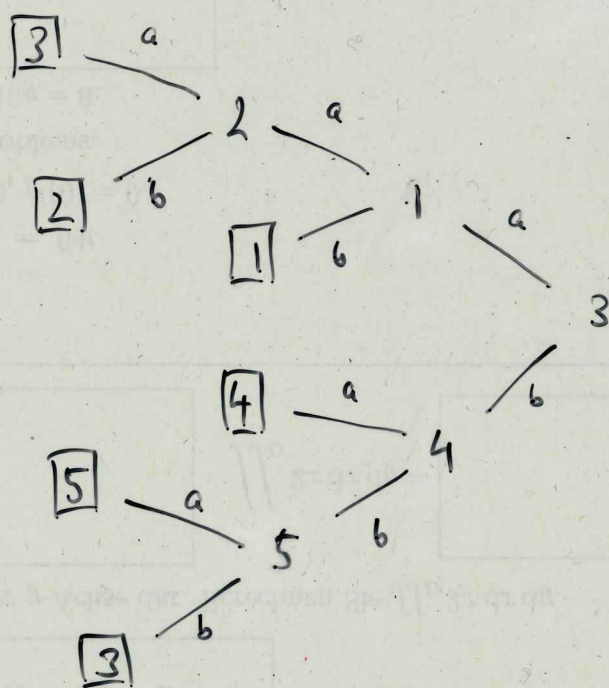
$$= \text{id}^{-1} \circ b^3 = \text{id}$$

$$\Rightarrow C_a(3) = \langle (2, 4, 5), (1, 2, 5), (1, 4, 5), (1, 2, 4) \rangle$$

$$\begin{aligned} & \textcircled{*} \langle (2, 4, 5), (1, 2, 5) \rangle \Rightarrow |G| = |C_a(3)| \cdot |G \cdot 3| = 60 \\ & \text{extra Rechnung} \rightarrow 12 \quad 5 \leftarrow \text{S.o.} \end{aligned}$$

Baum von rechts nach links

Kasten, falls schon vorher aufgeschrieben



$$\begin{aligned} & \textcircled{*} (1, 3, 5) \\ & (2, 4, 5) = (5, 4, 1) = (1, 4, 5) \\ & (1, 5, 2) (2, 4, 5) = (1, 4, 2) = (1, 2, 4) \\ & \leadsto (1, 4, 5), (1, 2, 4) \\ & \text{nicht benötigt} \end{aligned}$$

G : endl. Grp

p : Primzahl

$$a \in \mathbb{Z}_{\neq 0}, \quad a = p^k \cdot \frac{a'}{p^0} \quad \text{mit } a' \not\equiv 0$$

$$\Rightarrow a [p] := p^k$$

$$\text{Syl}_p(G) = \{ P \leq G : |P| = |G| [p] \}$$

Menge der p -Sylow untergruppen in G

Satz 38 (Sylow)

(1) $\text{Syl}_p(G) \neq \emptyset$

(2) $\text{Syl}_p(G)$ ist transitive G -Menge unter Konjugation

(3) $|\text{Syl}_p(G)| \equiv_p 1$

• Für $P \in \text{Syl}_p(G)$:

$$|\text{Syl}_p(G)| = \frac{|G|}{|N_G(P)|}, \quad \text{was } \frac{|G|}{|G| [p]} \text{ teilt}$$

(4) $U \leq G$ p -Untergruppe

$\Rightarrow \exists P \in \text{Syl}_p(G)$ mit $U \leq P$

Bsp Sei $|G| = 30$.

$$|\text{Syl}_5(G)| \equiv_5 1 \quad \text{und} \quad |\text{Syl}_5(G)| \text{ teilt } \frac{30}{30/5} = 6$$

$$\Rightarrow |\text{Syl}_5(G)| \in \{1, 6\}.$$

G : Gruppe

Lemma 4.3 (Iwasawa - Kriterium)

$\pi = (\pi, \alpha)$: primitive G -Rang

$m \in \pi$

$$\begin{array}{c} \uparrow \\ G \xrightarrow{\alpha} S_m \end{array}$$

$m \in \pi$

$K := \text{Kern}(\alpha)$

$C := C_G(m)$

$A \trianglelefteq C$ und A abelsch
und $G \triangleleft A \triangleleft G$.

Normalteilererzeugnis

$$G \triangleleft A \triangleleft G = \langle \bigcup_{g \in G} gAg^{-1} \rangle \trianglelefteq G$$

$[a, b] = a^{-1}b^{-1}ab$

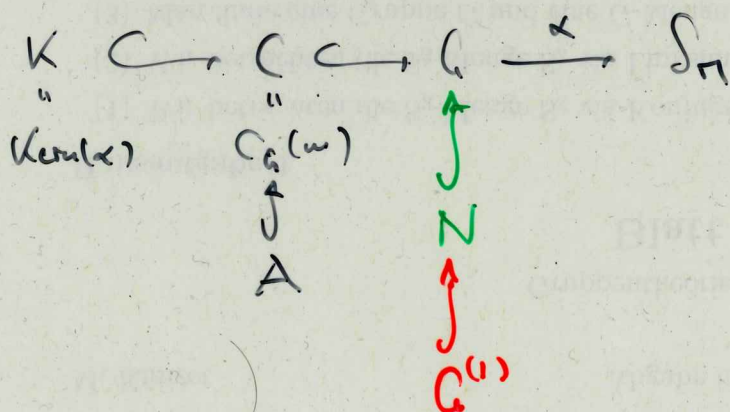
$G^{(1)} = [G, G] \trianglelefteq G$

Kommutatoruntergruppe

(1) $N \trianglelefteq G$ und $N \not\subseteq K$. Dann $G^{(1)} \leq N$

(2) G perfekt $\Rightarrow G/K$ einfach
 $G^{(1)} = G$ hat nur
Normalteiler
1 und G/K

Situation:



Nichtabelsche einfache Gruppen:

z.B.:

• $A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = +1\}$
ist eine einfache Gruppe für $n \geq 5$

• $PSL_n(F) = SL_n(F) / Z(SL_n(F))$
für einen Körper F , für $n \geq 2$,
vorausgesetzt $(n, |F|) \notin \{(2, 2), (2, 3)\}$,
ist eine einfache Gruppe

Berechnung von Ordnungen:

• $|A_5| = \frac{1}{2} \cdot 5! = 60$

$|A_6| = \frac{1}{2} \cdot 6! = 360$

• $|PSL_2(\mathbb{F}_7)| = \frac{|SL_2(\mathbb{F}_7)|}{|Z(SL_2(\mathbb{F}_7))|} = \frac{8 \cdot 42}{2} = 168$

$|SL_2(\mathbb{F}_7)| = \frac{|GL_2(\mathbb{F}_7)|}{|\mathbb{F}_7^\times|} = \frac{(49-1)(49-7)}{6} = 8 \cdot 42$

$Z(SL_2(\mathbb{F}_7)) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix} \right\}$ hat Ordnung 2

$\Rightarrow PSL_2(\mathbb{F}_7) \not\cong A_n$ für $n \geq 5$

Normalalgorithmus für Relationen

$G = \langle g_1, \dots, g_n \rangle$: endliche Gruppe

$\{\hat{g}_1, \dots, \hat{g}_n\}$: Menge mit n Elementen

$F = F(\{\hat{g}_1, \dots, \hat{g}_n\})$: freie Gruppe

$F \xrightarrow{\varphi} G : \hat{g}_i \mapsto g_i \text{ für } i \in \{1, \dots, n\}$

ist ein surjektiver Gruppenmorphismus.

$\text{Kern}(\varphi) = \underbrace{C_F(1_G)}_{\text{mit Normalalgorithmus berechenbar}} = \langle k_1, \dots, k_m \rangle$

$\Rightarrow \text{Kern}(\varphi) = F \triangleleft \underbrace{k_1, \dots, k_m}_{\text{häufig noch reduzierbar}} \triangleright$

$\Rightarrow F / \text{Kern}(\varphi)$

$= \underbrace{\langle \hat{g}_1, \dots, \hat{g}_n : \underbrace{r_1, \dots, r_m}_{\text{Relationen}} \rangle}_{\substack{\text{Erzeuger} \\ \text{endliche präsentische Gruppe}}} \xrightarrow{\sim} G$